

**PROTEKSI INTEGRITAS DATA DENGAN METODE CRC32 DAN SHA-256  
PADA APLIKASI PENGUNDUH DAN TRANSFER FILE**

Oleh

Bagus Pradipta Satriyajati Hutomo

NIM: 622013007



Skripsi

Untuk melengkapi salah satu syarat memperoleh  
Gelar Sarjana Teknik

Program Studi Sistem Komputer  
Fakultas Teknik Elektronika dan Komputer  
Universitas Kristen Satya Wacana Salatiga

Desember 2017

**PROTEKSI INTEGRITAS DATA DENGAN METODE CRC32 DAN SHA-256  
PADA APLIKASI PENGUNDUH DAN TRANSFER FILE**

Oleh

Bagus Pradipta Satriyajati Hutomo

NIM: 622013007

Skripsi ini telah diterima dan disahkan  
Untuk melengkapi salah satu syarat memperoleh

Gelar Sarjana Teknik

dalam

Konsentrasi Jaringan Komputer dan Telekomunikasi

Program Studi Sistem Komputer

Fakultas Teknik Elektronika Dan Komputer

Universitas Kristen Satya Wacana

Salatiga

1956

Disahkan oleh

Pembimbing I

Pembimbing II



Hartanto Kusuma Wardana, M.T.

Tgl. 31/1/18



Banu Wirawan Yohanes, M.CompSc.

Tgl. 1-2-2018



## PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : Bagus Pradipta Satriyagati Hutomo  
NIM : 622013007 Email : 622013007@student.uksw.edu  
Fakultas : FTEK Program Studi : Sistem Komputer  
Judul tugas akhir : Proteksi Integritas Data dengan Metode CRC32 dan SHA-256 pada Aplikasi Pengunduh dan Transfer File  
Pembimbing : 1. Hartanto Kusuma Wardana, M.T.  
2. Banu Wirawan Yohanes, M. CompSc.

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 31 Januari 2018



Tanda tangan dan cap resmi

Bagus Pradipta Satriyagati H.





## PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Bagus Pradipta Satriyagati Hutomo  
NIM : 622013007 Email : 622013007@student.uksw.edu  
Fakultas : FTEK Program Studi : Sistem Komputer  
Judul tugas akhir : Protoksi Integritas Data dengan Metode CRC32 dan SHA-256  
pada Aplikasi Pengunduh dan Transfer File

Dengan ini saya menyerahkan hak *non-eksklusif*\* kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

- ☒ a. Saya mengizinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA
- ☐ b. Saya tidak mengizinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA\*\*

\* Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-eksklusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.

\*\* Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 31 Januari 2019

Bagus Pradipta Satriyagati H.

Tanda tangan & nama terang mahasiswa

Mengetahui,

Hartanto Kusuma Wordana, M.T.

Tanda tangan & nama terang pembimbing I

Bnu Wirawan Yohanes, M.Comp.Sc.

Tanda tangan & nama terang pembimbing II

## INTISARI

Seiring file yang tersebar luas di internet, dibutuhkan perangkat lunak untuk mengecek integritas dan keamanan data setelah file diunduh atau ditransfer. Selain unduh dan transfer cek integritas juga dilakukan saat pengiriman file penting seperti dokumen. Untuk melakukan cek integritas dan keamanan data, digunakan nilai CRC32 dan SHA-256. Metode yang digunakan adalah dengan membangkitkan nilai CRC dan SHA saat pembuatan file khusus sebelum file diunggah. File yang diunduh atau transfer dicek dengan cara membandingkan nilai CRC dan SHA yang terdapat pada file, dan nilai CRC dan SHA yang dihitung oleh perangkat lunak. CRC32 dan SHA-256 dapat mendeteksi perubahan 1 bit pada file, sehingga CRC32 dan SHA-256 mampu untuk memeriksa integritas dan keamanan data.

Mengetahui,

Mengesahkan,

Penyusun,

Hartanto K. Wardana, M.T.

Hartanto K. Wardana, M.T.

Bagus Pradipta S.H.

Dekan

Pembimbing

## ABSTRACT

As files are widespread on the internet, software is required to check the integrity and security of data after the files are downloaded or transferred. In addition to download and transfer integrity checks are also done when sending important files such as documents. To perform these checks, CRC32 and SHA-256 values were used. The method is to generate CRC and SHA values when creating a special file before the files were uploaded. Downloaded or transferred files were checked by comparing the CRC and SHA values which these are contained in the file and the CRC and SHA values which were calculated by the software. CRC32 and SHA-256 can detect 1 bit changes in files, so CRC32 and SHA-256 are able to check data integrity and security.

## KATA PENGANTAR

Puji Syukur kepada Allah Bapa karena atas berkat yang melimpah, skripsi ini mampu diselesaikan. Dimulai tahun 2013 saat memulai awal kuliah hingga membuat skripsi ini, banyak pengalaman yang sudah dijadikan pelajaran, semua karena penyertaan Yesus Kristus Putramu.

Terima kasih pula kepada semua yang sudah mendukung secara langsung maupun tidak langsung dalam penulisan skripsi ini. Penulis mengucapkan terima kasih kepada:

1. Hartanto Kusuma Wardana, M.T., sebagai Dekan Fakultas Teknik Elektro dan Komputer dan pembimbing I.
2. Banu Wirawan Yohanes, M.ComSc., sebagai pembimbing II.
3. Seluruh Dosen dan Staf Fakultas Teknik Elektro dan Komputer.
4. Kedua orang tua yang saya cintai, yang sudah mendukung hingga kini. Juga kepada keluarga semuanya.
5. Teman-teman angkatan 2013, khususnya penghuni *channel* Discord yang sudah menggarani dan rela digarani.

## DAFTAR ISI

INTISARI .....	i
ABSTRACT.....	ii
KATA PENGANTAR .....	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR.....	vii
DAFTAR TABEL.....	xi
DAFTAR LAMBANG .....	xii
DAFTAR SINGKATAN .....	xiii
BAB I PENDAHULUAN.....	1
1.1. Tujuan .....	1
1.2. Latar Belakang .....	1
1.3. Gambaran Sistem .....	2
1.4. Spesifikasi Sistem .....	3
1.5. Sistematika Penulisan.....	4
BAB II DASAR TEORI .....	5
2.1. Jenis Perubahan pada File .....	5
2.2 .CRC.....	6
2.3. SHA-2 .....	7
2.4. <i>Hypertext Transfer Protocol</i> .....	12
2.5. <i>File Transfer Protocol</i> .....	12
2.6. <i>Windows file sharing</i> .....	13
2.7. Visual Studio 2017.....	13
BAB III PERANCANGAN .....	14
3.1. Perhitungan CRC .....	14
3.1.1. Perhitungan.....	15
3.2. Perhitungan SHA .....	16
3.2.1. Fungsi dan Konstanta .....	16
3.2.2. <i>Preprocessing</i> .....	16
3.2.3. Perhitungan.....	18



3.3. Pembuat File .....	20
3.3.1. Pembuat File SHA.....	20
3.3.2. Penggabung File.....	21
3.3.3. Pemberi CRC pada Nama File .....	22
3.3.4. Antarmuka.....	23
3.4. Pengunduh File .....	23
3.4.1. Unduh File.....	24
3.4.2. Cek CRC .....	26
3.4.3. Pemisah File .....	27
3.4.4. Cek SHA .....	28
3.4.5. Antarmuka.....	30
3.5. Aplikasi Transfer File ( <i>Server</i> ) .....	32
3.5.1. Pemecah File .....	33
3.5.2. Pembuat File SHA Setiap Segmen.....	34
3.5.3. Penggabung File.....	36
3.5.4. Pemberi CRC pada Nama File .....	36
3.5.5. Antarmuka.....	37
3.6. Aplikasi Transfer File ( <i>Client</i> ).....	38
3.6.1. Transfer File .....	39
3.6.2. Cek CRC .....	40
3.6.3. Pemisah File .....	42
3.6.4. Cek SHA .....	42
3.6.5. Penyatu Semua Segmen .....	44
3.6.6. Antarmuka.....	45
BAB IV PNEGUJIAN DAN ANALISIS .....	47
4.1. Pengujian Pembuat File .....	48
4.2. Pengujian Pengunduh File serta Analisa Cek CRC dan SHA .....	51
4.3. Pengujian Transfer File serta Analisa Cek CRC dan SHA .....	55
4.3.1. Pengujian pada <i>Server</i> .....	55
4.3.2. Pengujian pada <i>Client</i> .....	60
BAB V KESIMPULAN DAN SARAN .....	67

5.1. Kesimpulan .....	67
5.2. Saran.....	67
DAFTAR PUSTAKA .....	68
LAMPIRAN.....	70



## DAFTAR GAMBAR

Gambar 2.1. <i>Single-Bit Error</i> .....	5
Gambar 2.2. <i>Burst Error</i> .....	6
Gambar 2.3. Mencari <i>Checksum</i> dengan CRC 3-bit.....	7
Gambar 2.4. Cek CRC32 menggunakan Anime Checker .....	7
Gambar 2.5. Cek SHA-256 Menggunakan Open-Hashtool .....	8
Gambar 2.6. Urutan Perhitungan SHA .....	8
Gambar 2.7. SHA-256 <i>Constans</i> .....	9
Gambar 2.8. Contoh <i>Padding Message</i> .....	9
Gambar 2.9. Nilai <i>Hash</i> Awal SHA-256 .....	10
Gambar 2.10. Hasil <i>hash</i> “FTEK” online .....	11
Gambar 2.11. Ilustrasi Perhitungan SHA-256 .....	12
Gambar 3.1. Diagram Blok Aplikasi .....	14
Gambar 3.2. Diagram Alir Perhitungan CRC.....	15
Gambar 3.3. Diagram Alir Inisialisasi Fungsi dan Konstanta .....	16
Gambar 3.4. Diagram Alir Padding .....	17
Gambar 3.5. Diagram Alir Parsing dan Inisialisasi Hash Awal .....	18
Gambar 3.6. Diagram Alir Perhitungan SHA.....	19
Gambar 3.7. Cara Kerja Pembuat File .....	20
Gambar 3.8. Diagram Alir Pembuat File .....	21
Gambar 3.9. Diagram Alir Penggabung File .....	22
Gambar 3.10. Diagram Alir Pemberi CRC pada Nama File .....	22
Gambar 3.11. Antarmuka Pembuat File .....	23
Gambar 3.12. Cara Kerja Pengunduh File .....	24
Gambar 3.13. Diagram Alir Unduh File .....	25
Gambar 3.14. Diagram Alir Proses Unduh.....	26
Gambar 3.15. Diagram Alir Cek CRC.....	27
Gambar 3.16. Diagram Alir Pemisah File .....	28
Gambar 3.17. Diagram Alir Cek SHA.....	29
Gambar 3.18. Antarmuka Pengunduh File .....	30

Gambar 3.19. Antarmuka <i>Input URL</i> .....	31
Gambar 3.20. Antarmuka Pengaturan Folder .....	31
Gambar 3.21. Antarmuka Unduh.....	32
Gambar 3.22. Cara Kerja Pada Server .....	33
Gambar 3.23. Diagram Alir Pemecah File .....	34
Gambar 3.24. Diagram Alir Pembuat File SHA.....	35
Gambar 3.25. Diagram Alir Penggabung File .....	36
Gambar 3.26. Diagram Alir Pemberi CRC pada Nama File .....	37
Gambar 3.27. Antarmuka Transfer File (Sever) .....	38
Gambar 3.28. Cara Kerja Pada Client.....	39
Gambar 3.29. Diagram Alir Transfer File .....	40
Gambar 3.30. Diagram Alir Cek CRC.....	41
Gambar 3.31. Diagram Alir Pemisah File .....	42
Gambar 3.32. Diagram Alir Cek SHA.....	43
Gambar 3.33. Diagram Alir Penyatu Segmen .....	45
Gambar 3.34. Antermuka pada Client .....	46
Gambar 4.1. Topologi untuk Pengujian.....	47
Gambar 4.2. Hasil dari Pembuat File dan Isi File Ekstensi “abc” .....	48
Gambar 4.3. Proteksi Jika File “abc” Diubah atau Rusak .....	49
Gambar 4.4. Single-bit Error .....	49
Gambar 4.5. Burst Error .....	50
Gambar 4.6. File Dokumen.....	51
Gambar 4.7. Perubahan pada File Dokumen .....	51
Gambar 4.8. Unduh dari FTP server dengan 1 Segmen .....	52
Gambar 4.9 Unduh dari Solidfiles dengan 2 Segmen.....	52
Gambar 4.10. Unduh dari Zippyshare dengan 4 Segmen .....	52
Gambar 4.11. Unduh dari Tusfiles dengan 8 Segmen .....	52
Gambar 4.12. Hasil cek CRC dari program.....	53
Gambar 4.13. Hasil cek CRC dari Anime Checker .....	53
Gambar 4.14. Hasil cek SHA dari program.....	54
Gambar 4.15. Hasil cek SHA dari Open-Hashtool.....	54

Gambar 4.16. Hasil Unduh Dokumen .....	54
Gambar 4.17. Hasil CRC pada Anime Checker .....	55
Gambar 4.18. Hasil SHA pada Open-Hashtool .....	55
Gambar 4.19. Kecepatan Unduh Internet .....	55
Gambar 4.20. Hasil dari Server .....	56
Gambar 4.21. Single-bit Error .....	56
Gambar 4.22. Burst Error .....	57
Gambar 4.23. Hasil dari Server .....	57
Gambar 4.24. Burst Error .....	58
Gambar 4.25. Single-bit Error .....	58
Gambar 4.26. Hasil dari Server .....	59
Gambar 4.27. Burst Error .....	60
Gambar 4.28. Single-bit Error .....	60
Gambar 4.29. Hasil dari Client .....	61
Gambar 4.30. Nilai CRC pada Anime Checker .....	61
Gambar 4.31. Nilai SHA pada Open-Hashtool.....	61
Gambar 4.32. Hasil pada Client.....	61
Gambar 4.33. Nilai CRC pada Anime Checker .....	62
Gambar 4.34. Nilai SHA pada Open-Hashtool.....	62
Gambar 4.35. Hasil dari Client .....	62
Gambar 4.36. Nilai CRC pada Anime Checker.....	62
Gambar 4.37. Nilai SHA pada Open-Hashtool.....	63
Gambar 4.38. Hasil pada Client.....	63
Gambar 4.39. Nilai CRC pada Anime Checker .....	63
Gambar 4.40. Nilai SHA pada Open-Hashtool.....	64
Gambar 4.41. Hasil dari Client .....	64
Gambar 4.42. Nilai CRC pada Anime Checker .....	64
Gambar 4.43. Nilai SHA pada Open-Hashtool.....	65
Gambar 4.44. Hasil pada Client.....	65
Gambar 4.45. Nilai CRC pada Anime Checker .....	66
Gambar 4.46. Nilai SHA pada Open-Hashtool.....	66



Gambar 4.47. Kecepatan Transfer .....	67
---------------------------------------	----



## DAFTAR TABEL

Tabel 2.1. <i>Representation</i> dan <i>Polynomial</i> pada CRC32 .....	6
---	---



## DAFTAR LAMBANG

$Ch(x,y,z)$	<i>choose</i> pada fungsi SHA-256
$Maj(x,y,z)$	<i>Major</i> pada fungsi SHA-256
$\Sigma_0(x)$	Sigma 0 pada fungsi SHA-256
$\Sigma_1(x)$	Sigma 1 pada fungsi SHA-256
$\sigma_0(x)$	sigma 0 pada fungsi SHA-256
$\sigma_1(x)$	sigma 1 pada fungsi SHA-256
$x, y, z$	Variabel pada fungsi SHA-256
$W$	Pesan pada SHA-256
$N$	Jumlah pesan pada SHA-256
$\wedge$	Operasi AND
$\oplus$	Operasi XOR
$\neg$	Operasi Not
$ROTR^n$	<i>Rotate right</i> sebanyak $n$ -bit $((x \gg n)   (x \ll w - n))$
$SHR^n$	<i>Shift right</i> sebanyak $n$ -bit $(x \gg n)$
$+$	<i>Addition modulo</i> $2^{32}$ , jika hasil penambahan melebihi 32-bit di-modulo $2^{32}$
$K$	Konstan
$l$	Panjang pesan untuk 1 blok pesan
$k$	Jumlah <i>padding</i> 0 bit
$H$	Nilai <i>hash</i>

## DAFTAR SINGKATAN

LAN	<i>Local Area Network</i>
CRC	<i>Cyclic Redundancy Check</i>
SHA	<i>Secure Hash Algorithm</i>
HTTP	<i>Hypertext Transfer Protocol</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
WWW	<i>World Wide Web</i>
TCP	<i>Transport Control Protocol</i>
FTP	<i>File Transfer Protocol</i>
SMB	<i>Server Message Block</i>
NetBIOS	<i>Network Basic Input/Output System</i>
URL	<i>Uniform Resource Locator</i>